

ON THE 2-RANKS OF A CLASS OF UNITALS

ROCCO TROMBETTI AND YUE ZHOU

ABSTRACT. Let \mathcal{U}_θ be a unital defined in a shift plane of odd order q^2 , which are constructed recently in [33]. In particular, when the shift plane is desarguesian, \mathcal{U}_θ is a special Buekenhout-Metz unital formed by a union of ovals. We investigate the dimensions of the binary codes derived from \mathcal{U}_θ . By using Kloosterman sums, we obtain a new lower bound on the aforementioned dimensions which improves Leung and Xiang's result [26, 27]. In particular, for $q = 3^m$, this new lower bound equals $\frac{2}{3}(q^3 + q^2 - 2q) - 1$ for even m and $\frac{2}{3}(q^3 + q^2 + q) - 1$ for odd m .

1. INTRODUCTION

Let m be an integer larger than or equal to 3. A *unital* of order m is a $2-(m^3 + 1, m + 1, 1)$ design, i.e. a set of $m^3 + 1$ points arranged into subsets of size $m + 1$ such that each pair of distinct points are contained in exactly one of these subsets.

Most of the known unitals can be embedded in a projective plane Π of order q^2 . In such a case, the *embedded unital* is a set \mathcal{U} of $q^3 + 1$ points such that each line of Π intersects \mathcal{U} in 1 or $q + 1$ points. When Π is the desarguesian projective plane $\text{PG}(2, q^2)$, the set of absolute points of a unitary polarity, or equivalently speaking, the rational points on a nondegenerate Hermitian curve form a *classical* unital. There are also non-classical unitals in $\text{PG}(2, q^2)$, for instance the Buekenhout-Metz unitals [9], as well as the unitals which can not be embedded in a projective plane, such as the Ree unitals [29]. Moreover, it is not necessary that the order of a unital is a prime power, for instance, the order of the unitals discovered in [5] equals 6.

Unitals also exist in non-desarguesian planes. For instance, there are unitals derived from unitary polarities in various translation planes and shift planes; see [1, 3, 13, 14, 20, 22]. Commutative semifield planes, as a special type of translation and shift planes, also contain the unitals, which are analogous to the Buekenhout-Metz ones in desarguesian planes; see [2, 38].

Recently in [33], the authors investigate the existence and properties of a special type of unitals \mathcal{U}_θ consisting of ovals in shift planes $\Pi(f)$ of odd orders in terms of planar functions f on \mathbb{F}_{q^2} . In particular, when the planar function $f(x) = x^2$, the shift plane $\Pi(f)$ is desarguesian and the unital \mathcal{U}_θ is exactly the one independently discovered by Hirschfeld and Szönyi [19] and by Baker and Ebert [6], which forms a special subclass of the Buekenhout-Metz unitals in desarguesian planes; see [33] or Section 2 for more details.

Generally, a *linear code* is an arbitrary subspace of a vector space over a field. The *dimension* of a linear code is the dimension of the corresponding subspace.

2010 *Mathematics Subject Classification.* 51A45, 12K10, 51A35, 11L05.

Key words and phrases. Unital; binary code; shift plane; Kloosterman sum.

Let \mathcal{U} be a unital, namely, a $(q^3 + 1, q + 1, 1)$ -design. For any prime number p , let $C_p(\mathcal{U})$ be the subspace spanned by the characteristic vectors of the blocks of \mathcal{U} in $\mathbb{F}_p^{q^3+1}$. Here the characteristic vector v^B of a subset B of the point set of \mathcal{U} , is the vector in $\mathbb{F}_p^{q^3+1}$ with coordinate 1 in those positions corresponding to the elements in B and with coordinate 0 in all other positions.

The dimension of $C_p(\mathcal{U})$ is also called the p -rank of the design \mathcal{U} . It is worth noting that, as a design, \mathcal{U} is of order $q^2 - 1$. By [4, Theorem 2.4.1], $C_p(\mathcal{U})$ is interesting only when $p \mid (q^2 - 1)$. In this paper, we consider in the value of $C_2(\mathcal{U}_\theta)$, where \mathcal{U}_θ is a unital in a shift plane $\Pi(f)$ of odd order constructed in [33]; see Section 2 too. As we mentioned previously, when $f(x) = x^2$, our unitals correspond to a special subclass of the Buekenhout-Metz unitals in desarguesian planes. Baker and Wantz made the following conjecture.

Conjecture 1.1. *When $f(x) = x^2$, $\dim C_2(\mathcal{U}_\theta) = q^3 - q + 1$.*

This conjecture can be found in [7, 12, 36]. In [26, 27], Leung and Xiang proved that $\dim C_2(\mathcal{U}_\theta) \geq (q^3 - q^2 + q)(1 - \frac{1}{p}) + \frac{q^2}{p}$, where $p = \text{char}(\mathbb{F}_q)$. The proof of this conjecture was claimed by Wu in a conference talk [35] with few details. Nevertheless, the proof has not appeared in the public domain yet since 2012.

This paper is organized as follows: We first briefly introduce shift planes and the unitals \mathcal{U}_θ constructed in [33]. Then we investigate the dimensions of the binary codes generated by the characteristic vectors of the blocks of the unitals \mathcal{U}_θ . In particular, for $q = 3^n$ and $f(x) = x^2$, we use Kloosterman sums to improve Leung and Xiang's result [26, 27] on the aforementioned dimension.

2. SHIFT PLANES AND UNITALS

A projective plane is called a *shift plane* if there exists a flag $((\infty), L_\infty)$ and a commutative collineation group which fixes $((\infty), L_\infty)$ and acts regularly on the set of points not lying on L_∞ as well as the set of lines not passing through (∞) . A finite shift plane of order q can be equivalently derived from abelian $(q, q, q, 1)$ -relative difference sets (RDS for short); see [15].

When q is odd, all known abelian $(q, q, q, 1)$ -RDSs are subsets of the group $(\mathbb{F}_q^2, +)$. Such a $(q, q, q, 1)$ -RDS is equivalent to a function $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$, such that $x \mapsto f(x+a) - f(x)$ is always a bijection for each nonzero a . This type of functions are called *planar functions* on \mathbb{F}_q , which were first investigated by Dembowski and Ostrom in [11]. As the counterpart, when $q = 2^n$, abelian $(q, q, q, 1)$ -RDSs only exist in C_4^n where C_4 is the cyclic group of order 4. These RDSs can also be equivalently illustrated by functions over \mathbb{F}_{2^n} , which can be found in [31, 37].

Let \mathbb{F} be a finite field of an odd order and f a planar function on \mathbb{F} . We define a projective plane $\Pi(f)$ as follows:

- **Points:** $(x, y) \in \mathbb{F} \times \mathbb{F}$ and (a) for $a \in \mathbb{F} \cup \{\infty\}$;
- **Lines:** $L_{a,b} := \{(x, f(x+a) - b) : x \in \mathbb{F}\} \cup \{(a)\}$ for all $(a, b) \in \mathbb{F} \times \mathbb{F}$,
 $N_a := \{(a, y) : y \in \mathbb{F}\} \cup \{(\infty)\}$ and $L_\infty := \{(a) : a \in \mathbb{F} \cup \{\infty\}\}$.

The points except for those on L_∞ are called the *affine points* of $\Pi(f)$. By removing the line L_∞ and the points on it, we get an affine plane.

The set of maps

$$T := \{\tau_{u,v} : \tau_{u,v}(x, y) = (x + u, y + v) : u, v \in \mathbb{F}\}$$

induces an abelian collineation group on $\Pi(f)$, and this group acts regularly on the affine points and all lines $\{L_{a,b} : a, b \in \mathbb{F}\}$. Thus $\Pi(f)$ is a shift plane. We call this collineation group the *shift group* of $\Pi(f)$.

When f can be written as a Dembowski-Ostrom polynomial, i.e. $f(x) = \sum a_{ij}x^{p^i+p^j}$ where $p = \text{char}(\mathbb{F})$, the plane $\Pi(f)$ is also a commutative semifield plane. Using the corresponding semifield multiplication, we can label the points and lines of $\Pi(f)$ in a different way. The intersection of the translation group and the shift group of $\Pi(f)$ is $\{(x, y) \mapsto (x, y + b) : b \in \mathbb{F}\}$. See [17, Section 4] for details. We refer to [25] and [30] for recent surveys on semifields and planar functions respectively.

Up to equivalence, all known planar functions f on finite fields \mathbb{F}_q of odd characteristics can be written as a Dembowski-Ostrom polynomial except for the Coulter-Matthews ones which are power maps defined by $x \mapsto x^d$ on \mathbb{F}_{3^m} for certain d ; see [10]. Both the Dembowski-Ostrom planar functions and the Coulter-Matthews ones satisfy that

- $f(0) = 0$ and
- for arbitrary $a, b \in \mathbb{F}_q$, $f(a) = f(b)$ if and only if $a = \pm b$.

For a proof of the Dembowski-Ostrom polynomials case, we refer to [23]; for the Coulter-Matthews functions $f(x) = x^d$ on \mathbb{F}_{3^m} , it can be verified directly from the fact $\gcd(d, 3^m - 1) = 2$. Actually for a function f defined by a Dembowski-Ostrom polynomial, the above conditions are necessary and sufficient for f to be planar; see [34]. If a planar function satisfies the aforementioned two conditions, then we call it a *normal planar function*.

Let ξ be an element in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then every element x of \mathbb{F}_{q^2} can be written as $x = x_0 + x_1\xi$ where $x_0, x_1 \in \mathbb{F}_q$. Similarly, every function $f : \mathbb{F}_{q^2} \rightarrow \mathbb{F}_{q^2}$ can be written as $f(x) = f_0(x) + f_1(x)\xi$ where f_0, f_1 are maps from \mathbb{F}_q to itself. Throughout this paper, we frequently switch between the element $x \in \mathbb{F}_{q^2}$ and its two dimensional representation $(x_0, x_1) \in \mathbb{F}_q^2$. If a special assumption on ξ is needed, we will point it out explicitly.

In [33], it is proved that the set of points

$$(1) \quad \mathcal{U}_\theta := \{(x, t\theta) : x \in \mathbb{F}_{q^2}, t \in \mathbb{F}_q\} \cup \{(\infty)\}$$

is a unital in $\Pi(f)$ under the assumption that

$$\#\{x \in \mathbb{F}_{q^2} : \theta_1 f_0(x) - \theta_0 f_1(x) = c\} = \begin{cases} q + 1, & c \neq 0; \\ 1, & c = 0. \end{cases}$$

By choosing appropriate elements θ , it is shown that \mathcal{U}_θ are unitals for 8 distinct families of planar functions f ; see [33].

As a design, the point set of \mathcal{U}_θ is $\{(x, t\theta) : x \in \mathbb{F}_{q^2}, t \in \mathbb{F}_q\} \cup \{(\infty)\}$ and all of its blocks are

$$B_a := \{(a, t\theta) : t \in \mathbb{F}_q\} \cup \{(\infty)\},$$

for each $a \in \mathbb{F}_{q^2}$ and

$$B_{a,b} := \{(x, t\theta) : f(x + a) - b = t\theta, t \in \mathbb{F}_q\},$$

for each $a, b \in \mathbb{F}_{q^2}$ where $b_0\theta_1 - b_1\theta_0 \neq 0$. The equation $f(x + a) - b = t\theta$ is equivalent to the following two ones

$$\begin{aligned} f_0(x) - b_0 &= t\theta_0, \\ f_1(x) - b_1 &= t\theta_1. \end{aligned}$$

As $\theta \neq 0$, the above system of equations is equivalent to

$$\begin{aligned}\theta_1 f_0(x) - \theta_0 f_1(x) - (\theta_1 b_0 - \theta_0 b_1) &= 0, \\ f_1(x) - b_1 &= t\theta_1.\end{aligned}$$

(If $\theta_1 = 0$, then we replace the second equation by $f_0(x) - b_0 = t\theta_0$.) Hence, the block $B_{a,b}$ can also be written as

$$(2) \quad B_{a,b} = \left\{ \left(x, \frac{f_1(x+a) - b_1}{\theta_1} \cdot \theta \right) : f_0(x+a)\theta_1 - f_1(x+a)\theta_0 = b_0\theta_1 - b_1\theta_0 \right\},$$

where $b_0\theta_1 - b_1\theta_0 \neq 0$ and $\theta_1 \neq 0$. For $\theta_1 = 0$, we get

$$(3) \quad B_{a,b} = \left\{ \left(x, \frac{f_0(x+a) - b_0}{\theta_0} \cdot \theta \right) : f_0(x+a)\theta_1 - f_1(x+a)\theta_0 = b_0\theta_1 - b_1\theta_0 \right\}.$$

There are totally $q^4 - q^3 + q^2$ blocks and each of them contains $q+1$ points. For each pair of points, there is exactly one block containing them both. Hence \mathcal{U}_θ is a $2-(q^3+1, q+1, 1)$ -design.

It is not difficult to directly verify the following property of \mathcal{U}_θ .

Proposition 2.1. *Let \mathcal{U}_θ be a unital defined by (1). The subgroup $T_\theta := \{\tau_{a,b\theta} : a \in \mathbb{F}_{q^2}, b \in \mathbb{F}_q\}$ of the shift group T of $\Pi(f)$ acts regularly on the affine points of \mathcal{U}_θ .*

An oval \mathcal{O} in a projective plane Π of odd order q is a set of $q+1$ points such that every line in Π meets \mathcal{O} in 0, 1 or 2 points. According to the famous result by Segre in [32], all ovals in desarguesian planes of odd orders are nondegenerate conics. The following property of \mathcal{U}_θ is proved in [33]:

Proposition 2.2. *Let f be a normal planar function on \mathbb{F}_{q^2} and \mathcal{U}_θ be a unital in $\Pi(f)$ defined by (1). Then for each $c \in \mathbb{F}_{q^2}$, the set*

$$\mathcal{O}_c := \{(x, c) : x \in \mathbb{F}_{q^2}\} \cup \{(\infty)\}$$

is an oval in $\Pi(f)$ and \mathcal{U}_θ is a union of ovals, i.e.

$$\mathcal{U}_\theta = \bigcup_{t \in \mathbb{F}_q} \mathcal{O}_{t\theta}.$$

In particular, when $f(x) = x^2$ on \mathbb{F}_{q^2} , $\Pi(x^2)$ is a desarguesian plane and the following results hold:

Lemma 2.3. *Let θ be in \mathbb{F}_{q^2} such that θ^{q+1} is a nonsquare element in \mathbb{F}_q .*

- (1) *The set of points \mathcal{U}_θ defined by (1) is a unital of order q in the plane $\Pi(x^2)$ [33, Theorem 2.4].*
- (2) *All the unitals in $\{\mathcal{U}_\theta : \theta^{q+1} \text{ is a nonsquare in } \mathbb{F}_q\}$ are equivalent under the collineations of $\Pi(x^2)$ [33, Proposition 3.3].*
- (3) *The unital \mathcal{U}_θ is exactly the one constructed by Hirschfeld and Szönyi [19] and by Baker and Ebert [6] independently [33, Remark 1].*

3. BINARY CODES OF \mathcal{U}_θ AND THEIR DIMENSIONS

By using MAGMA [8] programs, we verified that for every planar functions on \mathbb{F}_{q^2} constructed in [33] with $q \leq 9$, the 2-ranks of all unitals \mathcal{U}_θ equal to $q^3 - q + 1$. Hence it seems that Conjecture 1.1 should also hold for other \mathcal{U}_θ , i.e. $\dim C_2(\mathcal{U}_\theta) = q^3 - q + 1$ holds for all unitals \mathcal{U}_θ defined by (1).

The following upper bound on the dimension of $C_2(\mathcal{U}_\theta)$ was first proved for $f(x) = x^2$ (See [26, 27] and [7, Theorem 6.23]), and it can be generalized to all the unitals \mathcal{U}_θ constructed in [33].

Proposition 3.1. *Let f be a normal planar function on \mathbb{F}_{q^2} and \mathcal{U}_θ a unital defined by (1). The characteristic vectors $v^{\mathcal{O}_{t\theta}}$ for all $t \in \mathbb{F}_q$, are linearly independent in $C_2(\mathcal{U}_\theta)^\perp$. Moreover, $\dim C_2(\mathcal{U}_\theta) \leq q^3 - q + 1$.*

Proof. A vector w lies in the dual of the binary code $C_2(\mathcal{U}_\theta)$ if and only if each block of \mathcal{U}_θ meets the support of w in an even number of points. Here the support of w is the set of points which correspond to the positions at which w is nonzero. For every block B_a of \mathcal{U}_θ containing (∞) , it meets $\mathcal{O}_{t\theta}$ in exactly two points. For every block $B_{a,b}$ of \mathcal{U}_θ , it meets $\mathcal{O}_{t\theta}$ in 0 or 2 points. Since $\mathcal{U}_\theta = \bigcup_{t \in \mathbb{F}_q} \mathcal{O}_{t\theta}$, all $v^{\mathcal{O}_{t\theta}} \in C_2(\mathcal{U}_\theta)^\perp$. As all these ovals have only the point (∞) in common, $\{v^{\mathcal{O}_{t\theta}} : t \in \mathbb{F}_q\}$ are linearly independent. It implies that $\dim(C_2(\mathcal{U}_\theta)^\perp) \geq q$. Therefore $\dim C_2(\mathcal{U}_\theta) \leq q^3 - q + 1$. \square

Instead of considering $\dim C_2(\mathcal{U}_\theta)$, we remove the point (∞) from the point set of \mathcal{U}_θ and each block B_a . The new incidence structure is denoted by \mathcal{U}'_θ . In other words, $C_2(\mathcal{U}'_\theta)$ is the code $C_2(\mathcal{U}_\theta)$ punctured the coordinate corresponding to (∞) . From the proof of Proposition 3.1, we know that all $v^{\mathcal{O}_{t\theta}} \in C_2(\mathcal{U}_\theta)^\perp$, which implies that $v^{\{(\infty)\}} \notin C_2(\mathcal{U}_\theta)$. Hence

$$(4) \quad \dim C_2(\mathcal{U}_\theta) = \dim C_2(\mathcal{U}'_\theta).$$

Now we proceed to use the group characters approach applied in [26] to calculate $\dim C_2(\mathcal{U}'_\theta)$. By Proposition 2.1, the group T_θ acts transitively on all points of \mathcal{U}_θ except for (∞) . Hence we can identify each coordinate of $C_2(\mathcal{U}'_\theta)$ with the elements in T_θ . That means the point $(x, t\theta) \in \mathcal{U}_\theta$ corresponds to $(x, t\theta) \in T_\theta$. Under this identification, the code $C_2(\mathcal{U}'_\theta)$ becomes an ideal of the group ring $\mathbb{F}_2[T_\theta]$ and we can use the characters on G to calculate $\dim C_2(\mathcal{U}'_\theta)$.

First we have to extend \mathbb{F}_2 . Let \mathbb{K} be a finite extension of \mathbb{F}_2 such that a primitive p -th root of unity ε_p is in \mathbb{K} . It is well known that

$$\dim C_2(\mathcal{U}'_\theta) = \dim_{\mathbb{K}} C_2(\mathcal{U}'_\theta) = \#\{\chi \in \hat{T}_\theta : Me_\chi \neq 0\},$$

where M is the submodule generated by the blocks of the incidence structure \mathcal{U}'_θ , \hat{T}_θ is the character group of T_θ and $e_\chi = \frac{1}{|T_\theta|} \sum_{g \in T_\theta} \chi(g^{-1})g$; see [24, Page 277]. Here $Me_\chi \neq 0$ means that Me_χ is not the trivial submodule $\{0\}$, which implies there exists at least one element B in M such that $Be_\chi \neq 0$. In other words,

$$(5) \quad \dim C_2(\mathcal{U}'_\theta) = \#\mathcal{K}(\mathcal{U}_\theta),$$

where $\mathcal{K}(\mathcal{U}_\theta)$ is defined to be the set of $\chi \in \hat{T}_\theta$ such that there exists at least one block B of \mathcal{U}'_θ satisfying $\chi(B) \neq 0$.

As $T_\theta \cong (\mathbb{F}_q^3, +)$, each character $\chi \in \hat{T}_\theta$ can be written as

$$\chi_{u,v,w} : (x, t\theta) \mapsto \varepsilon_p^{\text{Tr}_{q/p}(ux_0 + vx_1 + wt)},$$

where $u, v, w, t \in \mathbb{F}_q$ and $x = (x_0, x_1) \in \mathbb{F}_q^2$. For $t \in \mathbb{F}_q$, we also define

$$\chi(t) = \varepsilon_p^{\text{Tr}_{q/p}(t)}.$$

That means $\chi_{u,v,w}(x, t\theta) = \chi(ux_0 + vx_1 + w\theta)$. The well known *orthogonal relation* is

$$(6) \quad \sum_{x \in \mathbb{F}_q} \chi(ax) = \begin{cases} 1, & a = 0; \\ 0, & a \neq 0. \end{cases}$$

Lemma 3.2. *Let f be a normal planar function on \mathbb{F}_{q^2} . Let \mathcal{U}_θ be a unital defined by (1). Then $\chi_{u,v,0} \in \mathcal{K}(\mathcal{U}_\theta)$ and $\chi_{0,0,w} \notin \mathcal{K}(\mathcal{U}_\theta)$ for each $u, v \in \mathbb{F}_q$ and $w \in \mathbb{F}_q^*$.*

Proof. Recall that we write $x = x_0 + x_1\xi$ for each $x \in \mathbb{F}_{q^2}$. Without loss of generality, we assume that $\theta_1 \neq 0$ (otherwise $\theta_0 \neq 0$, we replace θ_1 and f_1 by θ_0 and f_0 respectively in the rest of this proof). By (2), we have that

$$B_{a,b} = \left\{ \left(x, \frac{f_1(x+a) - b_1}{\theta_1} \cdot \theta \right) : f_0(x+a)\theta_1 - f_1(x+a)\theta_0 = b_0\theta_1 - b_1\theta_0 \right\},$$

where $b_0\theta_1 - b_1\theta_0 \neq 0$. Let $w' = w/\theta_1$. We denote

$$(7) \quad C_{a,\beta(b)} := \{x : f_0(x+a)\theta_1 - f_1(x+a)\theta_0 = \beta(b)\},$$

where $\beta(b) = b_0\theta_1 - b_1\theta_0 \neq 0$. It follows that

$$\begin{aligned} \chi_{u,v,w}(B_{a,b}) &= \sum_{x \in C_{a,\beta(b)}} \chi \left(ux_0 + vx_1 + w \cdot \frac{f_1(x+a) - b_1}{\theta_1} \right) \\ &= \chi(-w'b_1) \sum_{x \in C_{0,\beta(b)}} \chi(u(x_0 - a_0) + v(x_1 - a_1) + w'f_1(x)) \\ &= \chi(-ua_0 - va_1 - w'b_1) \sum_{x \in C_{0,\beta(b)}} \chi(ux_0 + vx_1 + w'f_1(x)), \\ \chi_{u,v,w}(B_a) &= \sum_{t \in \mathbb{F}_q} \chi(ua_0 + va_1 + wt). \end{aligned}$$

When $u = v = 0$ and $w \neq 0$, by (6), we have

$$\chi_{0,0,w}(B_a) = \sum_{t \in \mathbb{F}_q} \chi(wt) = 0.$$

For each $c \in C_{0,\beta(b)}$, from the normality of f it follows that $c \neq 0$, $-c \in C_{0,\beta(b)}$ and $f_1(c) = f_1(-c)$. Hence

$$\chi_{0,0,w}(B_{a,b}) = \chi(-w'b_1) \sum_{x \in C_{0,\beta(b)}} \chi(w'f_1(x)) = 0.$$

That means $\chi_{0,0,w} \notin \mathcal{K}(\mathcal{U}_\theta)$.

When $w = 0$, we have

$$\chi_{u,v,0}(B_a) = \sum_{t \in \mathbb{F}_q} \chi(ua_0 + va_1) = q\chi(ua_0 + va_1) = \chi(ua_0 + va_1).$$

Therefore $\chi_{u,v,0} \in \mathcal{K}(\mathcal{U}_\theta)$. □

In the rest of this paper, we restrict ourselves to several special cases of f . The following theorem applies to the planar functions $f(x) = x^2$, the one derived from Dickson's semifields and the semifields constructed in [39]. In fact, for $f(x) = x^2$, this result is proved by Leung and Xiang in [26, 27] in a slightly different way.

Theorem 3.3. *Let f be a normal planar function on \mathbb{F}_{q^2} . Let \mathcal{U}_θ be a unital defined by (1). Assume that $\theta_1 \neq 0$ and $f_1(x) = 2x_0x_1$. If $w \neq 0$ and $\text{Tr}_{q/p}(\frac{uv}{w}\theta_1) \neq 0$, then $\chi_{u,v,w} \in \mathcal{K}(\mathcal{U}_\theta)$. Furthermore $\dim C_2(\mathcal{U}_\theta) \geq (q^3 - q^2 + q)\left(1 - \frac{1}{p}\right) + \frac{q^2}{p}$.*

Proof. From the proof of Lemma 3.2, we have $w' = w/\theta$ and

$$\chi_{u,v,w/2}(B_{a,b}) = \chi(-ua_0 - va_1 - w'b_1/2) \sum_{x \in C_{0,\beta(b)}} \chi(ux_0 + vx_1 + w'f_1(x)/2).$$

Hence we may only concentrate on the blocks $B_{0,b}$ and we denote $\sum_{x \in C_{0,\beta(b)}} \chi(ux_0 + vx_1 + w'f_1(x)/2)$ by $S(\beta)$. We then have

$$\begin{aligned} \sum_{\beta \in \mathbb{F}_q^*} S(\beta) &= \sum_{\beta \in \mathbb{F}_q^*} \sum_{x \in C_{0,\beta}} \chi(ux_0 + vx_1 + w'x_0x_1) \\ &= \sum_{x \in \mathbb{F}_{q^2}^*} \chi(ux_0 + vx_1 + w'x_0x_1) \\ &= \sum_{x_0 \in \mathbb{F}_q} \chi(ux_0) \sum_{x_1 \in \mathbb{F}_q} \chi((v + w'x_0)x_1) - \chi(0) \\ &= \chi\left(\frac{uv}{w'}\right) - \chi(0) \quad (\text{by (6)}) \\ &= \chi\left(\frac{uv}{w'}\right) + 1, \end{aligned}$$

which equals 0 if and only if $\text{Tr}_{q/p}(\frac{uv}{w'}) = 0$. If $\sum_{\beta \in \mathbb{F}_q^*} S(\beta) \neq 0$, then there is at least one nonzero term which means $\chi_{u,v,w} \in \mathcal{K}(\mathcal{U}_\theta)$.

To get the lower bound for $\mathcal{K}(\mathcal{U}_\theta)$, we need to count the cardinality of the set $\{(u, v, w) : w \neq 0, \text{Tr}_{q/p}(\frac{uv}{w}\theta_1) = 0\}$, which equals $(q-1)^2(1 + \frac{q}{p})$. Together with (4), (5) and Lemma 3.2, we have

$$\begin{aligned} \dim C_2(\mathcal{U}_\theta) &= \#\mathcal{K}(\mathcal{U}_\theta) \\ &\geq q^2 + \left((q-1)(q^2-1) - (q-1)^2\left(1 + \frac{q}{p}\right)\right) \\ &= (q^3 - q^2 + q)\left(1 - \frac{1}{p}\right) + \frac{q^2}{p}. \quad \square \end{aligned}$$

4. A NEW LOWER BOUND ON THE DIMENSION OF $C_2(\mathcal{U}_\theta)$

In this section, we proceed to improve the lower bound on $\mathcal{K}(\mathcal{U}_\theta)$ for $f(x) = x^2$. In the proof of our theorem, we need the following lemmas.

Lemma 4.1. [28, Theorem 6.26] *Let f be a nondegenerate quadratic form over \mathbb{F}_q , q odd, in an even number n of indeterminates. Then for $b \in \mathbb{F}_q$ the number of solutions of the equation $f(x_1, \dots, x_n) = b$ in \mathbb{F}_{q^n} is*

$$q^{n-1} + v(b)q^{(n-2)/2}\eta((-1)^{(n/2)}\Delta),$$

where η is the quadratic character of \mathbb{F}_q , $\Delta = \det(f)$ and the integer-valued function v is defined by $v(b) = -1$ for $b \in \mathbb{F}_q^*$ and $v(0) = q-1$.

Lemma 4.2. [28, Theorem 6.27] *Let f be a nondegenerate quadratic form over \mathbb{F}_q , q odd, in an odd number n of indeterminates. Then for $b \in \mathbb{F}_q$ the number of solutions of the equation $f(x_1, \dots, x_n) = b$ in \mathbb{F}_{q^n} is*

$$q^{n-1} + q^{(n-1)/2} \eta((-1)^{(n-1)/2} b \Delta),$$

where η is the quadratic character of \mathbb{F}_q and $\Delta = \det(f)$.

Lemma 4.3. *Let a be a nonzero element in \mathbb{F}_q . Then*

$$\sum_{c \in \mathbb{F}_q} \chi(ac^2) = 1.$$

Proof. As $(x, y) \mapsto \text{Tr}_{q/p}(a(x+y)^2) - \text{Tr}_{q/p}(ax^2) - \text{Tr}_{q/p}(ay^2)$ defines a nondegenerate bilinear form on \mathbb{F}_p^n , the function $x \mapsto \text{Tr}_{q/p}(ax^2)$ defines a nondegenerate quadratic form over \mathbb{F}_p . By Lemmas 4.1 and 4.2, we see that

$$\#\{x : \text{Tr}_{q/p}(ax^2) = b\} \equiv \begin{cases} 0 & (\text{mod } 2), \quad b \neq 0; \\ 1 & (\text{mod } 2), \quad b = 0. \end{cases}$$

Therefore $\sum_{c \in \mathbb{F}_q} \chi(ac^2) = \varepsilon_p^0 = 1$. \square

Let ζ_p be a primitive p -th root of unity in \mathbb{C} and \mathcal{O}_p the algebraic integer ring in $\mathbb{Q}(\zeta_p)$. The character function $\lambda : \mathbb{F}_q \rightarrow \mathbb{Q}[\zeta_p]$ is defined by $\lambda(x) = \zeta_p^{\text{Tr}_{q/p}(x)}$. As $\gcd(2, p) = 1$, it is well known that the ideal generated by 2 in \mathcal{O}_p can be uniquely factorized into prime ideals

$$(2) = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_g,$$

for certain g ; see [21, Chapter 13]. The following lemma is just a direct observation.

Lemma 4.4. *Let A be a finite multiset whose elements are in \mathbb{F}_q . In \mathbb{K} , the character sum $\sum_{c \in A} \chi(c) = 0$ if and only if there is a prime ideal \mathfrak{p}_i containing the ideal generated by 2 such that $\sum_{c \in A} \lambda(c) \in \mathfrak{p}_i$. In other words, $\sum_{c \in A} \chi(c) \neq 0$ if and only if $\sum_{c \in A} \lambda(c) \not\equiv 0 \pmod{2}$.*

Definition 4.5. For $a \in \mathbb{F}_q$, we define the *Kloostman sum* over \mathbb{F}_q by

$$K(a) := \sum_{x \in \mathbb{F}_q^*} \lambda(x^{-1} + ax).$$

It is worthy noting that in general the value of a Kloosterman sum $K(a)$ is always real, because the complex conjugate of it equals

$$\bar{K}(a) = \sum_{x \in \mathbb{F}_q^*} \lambda(-x^{-1} - ax) = \sum_{x \in \mathbb{F}_q^*} \lambda((-x)^{-1} + a(-x)) = K(a).$$

Next we proceed with our main result in this section. We take $f(x) = x^2$ for $x \in \mathbb{F}_{q^2}$. Let ω be a primitive element of \mathbb{F}_{q^2} . Depending on the value of q , we can choose θ in the following two ways such that θ^{q+1} is a nonsquare in \mathbb{F}_q .

- When -1 is a square in \mathbb{F}_q , i.e. $q \equiv 1 \pmod{4}$, we take $\xi = \omega^{(q+1)/2}$ and $\theta = \xi$. It is readily verified that ξ^2 and θ^{q+1} are both nonsquares in \mathbb{F}_q .
- When -1 is not a square in \mathbb{F}_q , i.e. $q \equiv 3 \pmod{4}$, we let $\xi \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $\xi^q = -\xi$. By Lemma 4.1 with $n = 2$, it is not difficult to show that there always exists $\theta_0 \in \mathbb{F}_q^*$ such that $\theta_0^2 - \alpha$ is a nonsquare. We take $\theta = \theta_0 + \xi$. It is clear that $\theta^{q+1} = \theta_0^2 - \alpha$ is a nonsquare.

By Lemma 2.3, we know that \mathcal{U}_θ is a unital in each of these two cases. Since all unitals \mathcal{U}_θ in $\Pi(x^2)$ are equivalent under certain collineations (see Lemma 2.3), we only have to handle with \mathcal{U}_θ where θ takes the aforementioned special values. In next theorem, we show a link between $S(\beta)$ and certain Kloosterman sums.

Theorem 4.6. *Let $u, v, w \in \mathbb{F}_q$ satisfying that $w \neq 0$ and $\text{Tr}_{q/p}(uv/w^2) = 0$. Let \mathcal{U}_θ be a unital embedded in $\Pi(x^2)$ defined in Lemma 2.3.*

- (a) *Assume that $q \equiv 1 \pmod{4}$. Let θ and ξ be both equal to $\omega^{(q+1)/2}$, where ω is a primitive element of \mathbb{F}_{q^2} . Let $\alpha = \xi^2$. Then $\chi_{u,v,w} \in \mathcal{K}(\mathcal{U}_\theta)$ if one of the following collections of conditions are satisfied:*
- $v = 0, u \neq 0$ and $K\left(-\frac{u^4}{64w^2} \cdot \alpha\right) \not\equiv 2 \pmod{4}$;
 - $u = 0, v \neq 0$ and $K\left(-\frac{v^4}{64w^2} \cdot \frac{1}{\alpha}\right) \not\equiv 2 \pmod{4}$.
- (b) *Assume that $q \equiv 3 \pmod{4}$. Let $\xi \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be such that $\xi^q = -\xi$ and $\theta = \theta_0 + \xi$, where θ_0 is such that $\theta_0^2 - \alpha$ is a nonsquare in \mathbb{F}_q . Then $\chi_{u,v,w} \in \mathcal{K}(\mathcal{U}_\theta)$ if one of the following collections of conditions are satisfied:*
- $v = 0, u \neq 0$ and $K\left(\frac{u^4}{64w^2} \cdot (\theta_0^2 - \alpha)\right) \not\equiv 0 \pmod{4}$;
 - $u = 0, v \neq 0$ and $K\left(\frac{v^4\alpha^2}{64w^2} \cdot (\theta_0^2 - \alpha)\right) \not\equiv 0 \pmod{4}$.

Proof. Let us first look at the expressions of $C_{0,\beta}$ (see (7)).

- When $q \equiv 1 \pmod{4}$, we have $\theta_0 = 0$ and $\theta_1 = 1$. Hence

$$(8) \quad C_{0,\beta} = \{(x_0, x_1) : x_0^2 + \alpha x_1^2 = \beta\}.$$

- When $q \equiv 3 \pmod{4}$, we have

$$(9) \quad C_{0,\beta} = \{(x_0, x_1) : x_0^2 - 2\theta_0 x_0 x_1 + \alpha x_1^2 = \beta\}.$$

As we take $f(x) = x^2$, $x \in C_{0,\beta}$ if and only if $-x \in C_{0,\beta}$. Hence we may define $C_{0,\beta}^{(+)}$ as a complete set of coset representatives of the subgroup $\{1, -1\}$ in $C_{0,\beta}$ and $C_{0,\beta}^{(-)} := C_{0,\beta} \setminus C_{0,\beta}^{(+)}$. Similarly for \mathbb{F}_q^* , we define $\mathbb{F}_q^{(+)}$ and $\mathbb{F}_q^{(-)}$. For convenience, we use \square_q to denote the square elements in \mathbb{F}_q^* .

Our idea is to investigate $\sum_{c \in \square_q} S(c)$ and $\sum_{c \in \mathbb{F}_q^* \setminus \square_q} S(c)$ respectively. If we can show that one of them is not zero, then there exists at least one $S(c) \neq 0$, which means that $\chi_{u,v,w} \in \mathcal{K}(\mathcal{U}_\theta)$.

First let us calculate $\sum_{c \in \square_q} S(c)$.

$$\begin{aligned} \sum_{c \in \square_q} S(c) &= \sum_{d \in \mathbb{F}_q^{(+)}} S(d^2) \\ &= \sum_{d \in \mathbb{F}_q^{(+)}} \sum_{x \in C_{0,d^2}} \chi(ux_0 + vx_1 + wx_0x_1). \end{aligned}$$

As the points in (8) and (9) are both defined by nondegenerate quadratic forms, it implies that,

$$\begin{aligned}
\sum_{c \in \square_q} S(c) &= \sum_{d \in \mathbb{F}_q^{(+)}} \sum_{x \in C_{0,1}} \chi(udx_0 + vdx_1 + wd^2x_0x_1) \\
&= \sum_{x \in C_{0,1}^{(+)}} \sum_{d \in \mathbb{F}_q^{(+)}} (\chi(udx_0 + vdx_1 + wd^2x_0x_1) \\
&\quad + \chi(-udx_0 - vdx_1 + wd^2x_0x_1)) \\
&= \sum_{x \in C_{0,1}^{(+)}} \sum_{d \in \mathbb{F}_q^*} \chi(udx_0 + vdx_1 + wd^2x_0x_1).
\end{aligned}$$

It is not difficult to verify that $(x_0, x_1) \in C_{0,1}$ is such that $x_0x_1 = 0$ if and only if $x_1 = 0$ and $x_0 = \pm 1$. Without loss of generality, we assume that $(1, 0) \in C_{0,1}^{(+)}$. Let $\mathbf{1}_0 : \mathbb{F}_q \rightarrow \{0, 1\}$ be a function defined by $\mathbf{1}_0(0) = 1$ and $\mathbf{1}_0(u) = 0$ if $u \neq 0$. We continue our calculation of $\sum_{c \in \square_q} S(c)$.

$$\begin{aligned}
&\sum_{x \in C_{0,1}^{(+)}} \sum_{d \in \mathbb{F}_q^*} \chi(udx_0 + vdx_1 + wd^2x_0x_1) \\
&= \sum_{\substack{x \in C_{0,1}^{(+)} \\ x_1 \neq 0}} \sum_{d \in \mathbb{F}_q^*} \chi \left(wx_0x_1 \left(d + \frac{ux_0 + vx_1}{2wx_0x_1} \right)^2 - \frac{(ux_0 + vx_1)^2}{4wx_0x_1} \right) + \sum_{d \in \mathbb{F}_q^*} \chi(ud) \\
&= \sum_{\substack{x \in C_{0,1}^{(+)} \\ x_1 \neq 0}} \sum_{c \neq \frac{ux_0 + vx_1}{2wx_0x_1}} \chi(wx_0x_1c^2) \chi \left(-\frac{(ux_0 + vx_1)^2}{4wx_0x_1} \right) + (\mathbf{1}_0(u) + 1) \\
&= \sum_{\substack{x \in C_{0,1}^{(+)} \\ x_1 \neq 0}} \left(\chi \left(-\frac{(ux_0 + vx_1)^2}{4wx_0x_1} \right) \sum_{c \in \mathbb{F}_q} \chi(wx_0x_1c^2) - \chi(0) \right) + (\mathbf{1}_0(u) + 1) \\
&= \sum_{\substack{x \in C_{0,1}^{(+)} \\ x_1 \neq 0}} \left(\chi \left(-\frac{(ux_0 + vx_1)^2}{4wx_0x_1} \right) - 1 \right) + (\mathbf{1}_0(u) + 1), \quad (\text{by Lemma 4.3}).
\end{aligned}$$

Since $\# \{x : x \in C_{0,1}^{(+)}, x_1 \neq 0\} = \frac{q-1}{2}$, we obtain

$$(10) \quad \sum_{c \in \square_q} S(c) = \sum_{\substack{x \in C_{0,1}^{(+)} \\ x_1 \neq 0}} \chi \left(-\frac{(ux_0 + vx_1)^2}{4wx_0x_1} \right) + \mathbf{1}_0(u) + \frac{q+1}{2}.$$

Similarly we can show that

$$(11) \quad \sum_{c \in \square_q} S(c\alpha) = \sum_{\substack{x \in C_{0,\alpha}^{(+)} \\ x_0 \neq 0}} \chi \left(-\frac{(ux_0 + vx_1)^2}{4wx_0x_1} \right) + \mathbf{1}_0(v) + \frac{q+1}{2}$$

Now we turn to the character sums over $\mathbb{Q}(\zeta_p)$. Using (8) and (9), we can verify that for (x_0, x_1) and $(y_0, y_1) \in C_{0,1}$ with $x_1, y_1 \neq 0$, $\frac{x_0}{x_1} = \frac{y_0}{y_1}$ if and only if $(x_0, x_1) = (y_0, y_1)$ or $(x_0, x_1) = (-y_0, -y_1)$. Hence

$$\begin{aligned}
& \sum_{\substack{x \in C_{0,1}^{(+)} \\ x_1 \neq 0}} \lambda \left(-\frac{(ux_0 + vx_1)^2}{4wx_0x_1} \right) \\
&= \sum_{\substack{x \in C_{0,1}^{(+)} \\ x_1 \neq 0}} \lambda \left(-\frac{u^2}{4w} \frac{x_0}{x_1} - \frac{v^2}{4w} \frac{x_1}{x_0} \right) \lambda \left(-\frac{uv}{2w} \right) \\
&= \frac{1}{2} \lambda \left(-\frac{uv}{2w} \right) \sum_{\substack{x \in C_{0,1} \\ x_1 \neq 0}} \lambda \left(-\frac{u^2}{4w} \frac{x_0}{x_1} - \frac{v^2}{4w} \frac{x_1}{x_0} \right) \\
(12) \quad &= \frac{1}{2} \sum_{\substack{x \in C_{0,1} \\ x_1 \neq 0}} \lambda \left(-\frac{u^2}{4w} \frac{x_0}{x_1} - \frac{v^2}{4w} \frac{x_1}{x_0} \right) \quad \left(\text{Tr}_{q/p} \left(\frac{uv}{w} \right) = 0 \right).
\end{aligned}$$

Similarly,

$$(13) \quad \sum_{\substack{x \in C_{0,\alpha}^{(+)} \\ x_0 \neq 0}} \lambda \left(-\frac{(ux_0 + vx_1)^2}{4wx_0x_1} \right) = \frac{1}{2} \sum_{\substack{x \in C_{0,\alpha} \\ x_0 \neq 0}} \lambda \left(-\frac{u^2}{4w} \frac{x_0}{x_1} - \frac{v^2}{4w} \frac{x_1}{x_0} \right).$$

Let us first consider the case in which $q \equiv 1 \pmod{4}$. In this case, $C_{0,\beta}$ is defined by (8) and we can parameterize the points in $C_{0,1}$ and $C_{0,\alpha}$ as follows:

$$(14) \quad C_{0,1} = \left\{ \left(\frac{1 - \alpha t^2}{1 + \alpha t^2}, \frac{2t}{1 + \alpha t^2} \right) : t \in \mathbb{F}_q^* \right\} \cup \{(\pm 1, 0)\},$$

$$(15) \quad C_{0,\alpha} = \left\{ \left(\frac{2\alpha t}{\alpha + t^2}, \frac{\alpha - t^2}{\alpha + t^2} \right) : t \in \mathbb{F}_q^* \right\} \cup \{(0, \pm 1)\}.$$

When $v = 0$ and $u \neq 0$, we continue the calculation of (12)

$$\begin{aligned}
& \frac{1}{2} \sum_{\substack{x \in C_{0,1} \\ x_1 \neq 0}} \lambda \left(-\frac{u^2}{4w} \frac{x_0}{x_1} - \frac{v^2}{4w} \frac{x_1}{x_0} \right) \\
&= \frac{1}{2} \sum_{\substack{x \in C_{0,1} \\ x_1 \neq 0}} \lambda \left(-\frac{u^2}{4w} \frac{x_0}{x_1} \right) \\
&= \frac{1}{2} \sum_{t \in \mathbb{F}_q^*} \lambda \left(-\frac{u^2}{4w} \frac{1 - \alpha t^2}{2t} \right) \\
&= \frac{1}{2} \sum_{t \in \mathbb{F}_q^*} \lambda \left(\frac{1}{t \left(-\frac{8w}{u^2} \right)} - \alpha \left(\frac{u^2}{8w} \right)^2 t \left(-\frac{8w}{u^2} \right) \right) \\
&= \frac{1}{2} K \left(-\frac{u^4}{64w^2} \cdot \alpha \right).
\end{aligned}$$

By (10), Lemma 4.4 and the above equation, we show that $\sum_{c \in \square_q} S(c) \neq 0$ if and only if

$$K\left(-\frac{u^4}{64w^2} \cdot \alpha\right) \not\equiv 2 \pmod{4}.$$

Similarly for $u = 0$ and $v \neq 0$, (13) becomes

$$\frac{1}{2} \sum_{\substack{x \in C_{0,\alpha} \\ x_0 \neq 0}} \lambda\left(-\frac{u^2}{4w} \frac{x_0}{x_1} - \frac{v^2}{4w} \frac{x_1}{x_0}\right) = \frac{1}{2} K\left(-\frac{v^4}{64w^2} \cdot \frac{1}{\alpha}\right).$$

By (11), Lemma 4.4 and the above equation, we see that $\sum_{c \in \square_q} S(c\alpha) \neq 0$ if and only if

$$K\left(-\frac{v^4}{64w^2} \cdot \frac{1}{\alpha}\right) \not\equiv 2 \pmod{4}.$$

Next let consider the case in which $q \equiv 3 \pmod{4}$. In this case, $C_{0,\beta}$ is defined by (9). Let $\tilde{\alpha} := \alpha - \theta_0^2$. We can parameterize the points in $C_{0,1}$ and $C_{0,\alpha}$ as follows:

$$(16) \quad C_{0,1} = \left\{ \left(\frac{1 - 2\theta_0 t - \tilde{\alpha} t^2}{1 + \tilde{\alpha} t^2}, \frac{2t}{1 + \tilde{\alpha} t^2} \right) : t \in \mathbb{F}_q^* \right\} \cup \{(\pm 1, 0)\},$$

$$(17) \quad C_{0,\alpha} = \left\{ \left(\frac{2t/\alpha}{1 + \tilde{\alpha} t^2}, \frac{1 - 2\theta_0 t/\alpha^2 - \tilde{\alpha} t^2}{1 + \tilde{\alpha} t^2} \right) : t \in \mathbb{F}_q^* \right\} \cup \{(0, \pm 1)\}.$$

When $v = 0$ and $u \neq 0$, (12) becomes

$$\begin{aligned} & \frac{1}{2} \sum_{\substack{x \in C_{0,1} \\ x_1 \neq 0}} \lambda\left(-\frac{u^2}{4w} \frac{x_0}{x_1} - \frac{v^2}{4w} \frac{x_1}{x_0}\right) \\ &= \frac{1}{2} \sum_{t \in \mathbb{F}_q^*} \lambda\left(-\frac{u^2}{4w} \frac{1 - \tilde{\alpha} t^2}{2t} + \frac{u^2}{4w} \theta_0\right) \\ &= \frac{1}{2} \lambda\left(\frac{u^2 \theta_0}{4w}\right) \sum_{t \in \mathbb{F}_q^*} \lambda\left(\frac{1}{t \left(-\frac{8w}{u^2}\right)} - \tilde{\alpha} \left(\frac{u^2}{8w}\right)^2 t \left(-\frac{8w}{u^2}\right)\right) \\ &= \frac{1}{2} \lambda\left(\frac{u^2 \theta_0}{4w}\right) K\left(-\frac{u^4}{64w^2} \cdot \tilde{\alpha}\right). \end{aligned}$$

From (10), Lemma 4.4 and the above equation, we deduce that $\sum_{c \in \square_q} S(c) \neq 0$ if and only if

$$K\left(-\frac{u^4}{64w^2} \cdot \tilde{\alpha}\right) \not\equiv 0 \pmod{4}.$$

Similarly for $u = 0$ and $v \neq 0$, (13) becomes

$$\frac{1}{2} \sum_{\substack{x \in C_{0,\alpha} \\ x_0 \neq 0}} \lambda\left(-\frac{u^2}{4w} \frac{x_0}{x_1} - \frac{v^2}{4w} \frac{x_1}{x_0}\right) = \frac{1}{2} \lambda\left(\frac{v^2 \theta_0 \theta_0}{4w\alpha}\right) K\left(-\frac{v^4 \alpha^2}{64w^2} \cdot \tilde{\alpha}\right).$$

Again, from (11), Lemma 4.4 and the above equation, we see that $\sum_{c \in \square_q} S(c\alpha) \neq 0$ if and only if

$$K\left(-\frac{v^4 \alpha^2}{64w^2} \cdot \tilde{\alpha}\right) \not\equiv 0 \pmod{4}. \quad \square$$

When u and v are both nonzero, from the proof of Theorem 4.6, we see that whether $\chi_{u,v,w}$ belongs $\mathcal{K}(\mathcal{U}_\theta)$ depends on the values of (12) and (13) modulo 4, which are in general difficult to determine. Even for the case in Theorem 4.6, it is quite difficult to determine $K(a) \pmod{4}$ for an arbitrary $a \in \mathbb{F}_q$. However, for $p = \text{char}(\mathbb{F}_q) = 3$, there are several interesting results.

Theorem 4.7. [16, 18] *Let $a \in \mathbb{F}_{3^m}$. Then exactly one of the following cases occurs:*

- (a) $a = 0$ or a is a square, $\text{Tr}_{3^m/3}(\sqrt{a}) \neq 0$ and $K(a) \equiv 1 \pmod{2}$.
- (b) $a = t^2 - t^3$ for some $t \in \mathbb{F}_{3^m} \setminus \{0, 1\}$, at least one of t and $1 - t$ is a square and $K(a) \equiv 2m + 2 \pmod{4}$. The number of $a \in \mathbb{F}_{3^m}^*$ such that $K(a) \equiv 2m + 2 \pmod{4}$ is $\frac{5}{12}q - \frac{5}{4}$ if m is odd, and $\frac{5}{12}q - \frac{3}{4}$ if m is even.
- (c) $a = t^2 - t^3$ for some $t \in \mathbb{F}_{3^m} \setminus \{0, 1\}$, both t and $1 - t$ are nonsquares and $K(a) \equiv 2m \pmod{4}$. The number of $a \in \mathbb{F}_{3^m}^*$ such that $K(a) \equiv 2m \pmod{4}$ is $\frac{1}{4}(q + 1)$ if m is odd, and $\frac{1}{4}(q - 1)$ if m is even.

By Theorems 4.6 and 4.7, we can improve the lower bound for $\mathcal{K}(\mathcal{U}_\theta)$ when q is a power of 3.

Corollary 4.8. *Let $q = 3^m$ and \mathcal{U}_θ a unital embedded in $\Pi(x^2)$ defined in Lemma 2.3. Then*

$$\dim C_2(\mathcal{U}_\theta) \geq \begin{cases} \frac{2}{3}(q^3 + q^2 - 2q) - 1, & m \text{ is even;} \\ \frac{2}{3}(q^3 + q^2 + q) - 1, & m \text{ is odd.} \end{cases}$$

Proof. When m is even, -1 is a square in \mathbb{F}_q . By Theorem 4.7 and the fact that α is a nonsquare, $K(-\frac{u^4}{64w^2} \cdot \alpha) \not\equiv 2 \pmod{4}$ if and only if $K(-\frac{u^4}{64w^2} \cdot \alpha) \equiv 0 \pmod{4}$. A similar result can be obtained for $K(-\frac{v^4}{64w^2} \cdot \frac{1}{\alpha})$. The cardinalities of the following two sets

$$\begin{aligned} & \left\{ (u, w) : w \neq 0, K\left(-\frac{u^4}{64w^2} \cdot \alpha\right) \equiv 0 \pmod{4} \right\}, \\ & \left\{ (v, w) : w \neq 0, K\left(-\frac{v^4}{64w^2} \cdot \frac{1}{\alpha}\right) \equiv 0 \pmod{4} \right\}, \end{aligned}$$

both equal to

$$2(q - 1) \# \{a \in \mathbb{F}_q : K(a) \equiv 0 \pmod{4}\} = \frac{1}{2}(q - 1)^2.$$

By Theorem 4.6, there are at least $2 \cdot \frac{1}{2}(q - 1)^2$ characters $\chi_{u,v,w} \in \mathcal{K}(\mathcal{U}_\theta)$ when one of u and v equals 0. Combining this result ($\text{Tr}_{q/p}(uv/w^2) = 0$) with the corresponding lower bound obtained in Theorem 3.3 ($\text{Tr}_{q/p}(uv\theta_1/w^2) \neq 0$ and $\theta_1 = 1$), we have

$$\begin{aligned} \#\mathcal{K}(\mathcal{U}_\theta) & \geq (q^3 - q^2 + q)(1 - \frac{1}{3}) + \frac{q^2}{3} + 2 \cdot \frac{1}{2}(q - 1)^2 \\ & = \frac{2}{3}(q^3 + q^2 - 2q) - 1. \end{aligned}$$

When m is odd, $\theta_0^2 - \alpha$ is a nonsquare. By Theorem 4.7, $K\left(\frac{u^4}{64w^2} \cdot (\theta_0^2 - \alpha)\right) \not\equiv 0 \pmod{4}$ if and only if $K\left(\frac{u^4}{64w^2} \cdot (\theta_0^2 - \alpha)\right) \equiv 2 \pmod{4}$ and a similar result can be obtained for $K\left(\frac{v^4\alpha^2}{64w^2} \cdot (\theta_0^2 - \alpha)\right)$. The cardinality of the following two sets

$$\left\{ (u, w) : w \neq 0, K\left(\frac{u^4}{64w^2} \cdot (\theta_0^2 - \alpha)\right) \equiv 2 \pmod{4} \right\},$$

$$\left\{ (v, w) : w \neq 0, K \left(\frac{v^4 \alpha^2}{64w^2} \cdot (\theta_0^2 - \alpha) \right) \equiv 2 \pmod{4} \right\},$$

both equal to

$$2(q-1) \# \{a \in \mathbb{F}_q : K(a) \equiv 2 \pmod{4}\} = \frac{1}{2}(q^2 - 1).$$

Again by Theorem 3.3 and Theorem 4.6, we have

$$\begin{aligned} \#K(\mathcal{U}_\theta) &\geq (q^3 - q^2 + q)(1 - \frac{1}{3}) + \frac{q^2}{3} + 2 \cdot \frac{1}{2}(q^2 - 1) \\ &= \frac{2}{3}(q^3 + q^2 + q) - 1. \end{aligned}$$

Together with (4) and (5), we get two lower bounds on $\dim C_2(\mathcal{U}_\theta)$. \square

ACKNOWLEDGMENT

The authors would like to thank Qing Xiang for pointing out the work of Junhua Wu [35]. This work is supported by the Research Project of MIUR (Italian Office for University and Research) “Strutture geometriche, Combinatoria e loro Applicazioni” 2012. Yue Zhou is partially supported by the National Natural Science Foundation of China (No. 11401579).

REFERENCES

- [1] V. Abatangelo, M. R. Enea, G. Korchmáros, and B. Larato. Ovals and unitals in commutative twisted field planes. *Discrete Mathematics*, 208–209:3–8, 1999.
- [2] V. Abatangelo, G. Korchmáros, and B. Larato. Transitive parabolic unitals in translation planes of odd order. *Discrete Mathematics*, 231(1–3):3–10, Mar. 2001.
- [3] V. Abatangelo and B. Larato. Polarity and transitive parabolic unitals in translation planes of odd order. *Journal of Geometry*, 74(1–2):1–6, Nov. 2002.
- [4] E. F. Assmus and J. D. Key. *Designs and Their Codes*. Cambridge University Press, Aug. 1992.
- [5] S. Bagchi and B. Bagchi. Designs from pairs of finite fields. A cyclic unital $U(6)$ and other regular steiner 2-designs. *Journal of Combinatorial Theory, Series A*, 52(1):51–61, Sept. 1989.
- [6] R. D. Baker and G. L. Ebert. Intersection of unitals in the Desarguesian plane. In *Congressus Numerantium. A Conference Journal on Numerical Themes*, volume 70, pages 87–94, 1990.
- [7] S. Barwick and G. Ebert. *Unitals in Projective Planes*. Springer Monographs in Mathematics. Springer New York, Jan. 2008.
- [8] W. Bosma, J. Cannon, and C. Playoust. The MAGMA algebra system I: the user language. *J. Symb. Comput.*, 24(3–4):235–265, 1997.
- [9] F. Buekenhout. Characterizations of semi quadrics. *Atti Conv. Lincei*, 17:393–421, 1976.
- [10] R. S. Coulter and R. W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Des. Codes Cryptography*, 10(2):167–184, 1997.
- [11] P. Dembowski and T. G. Ostrom. Planes of order n with collineation groups of order n^2 . *Mathematische Zeitschrift*, 103:239–258, 1968.
- [12] G. Ebert. Binary codes of odd order bukenhout-metz unitals. talk given in Oberwolfach, December 2001.
- [13] M. J. Ganley. A class of unitary block designs. *Mathematische Zeitschrift*, 128(1):34–42, Mar. 1972.
- [14] M. J. Ganley. Polarities in translation planes. *Geometriae Dedicata*, 1(1):103–116, 1972.
- [15] M. J. Ganley and E. Spence. Relative difference sets and quasiregular collineation groups. *Journal of Combinatorial Theory. Series A*, 19(2):134–153, 1975.
- [16] K. Garaschuk and P. Lisoněk. On ternary Kloosterman sums modulo 12. *Finite Fields and their Applications*, 14(4):1083–1090, 2008.

- [17] D. Ghinelli and D. Jungnickel. Finite projective planes with a large abelian group. In *Surveys in combinatorics, 2003 (Bangor)*, volume 307 of *London Math. Soc. Lecture Note Ser.*, page 175–237. Cambridge Univ. Press, Cambridge, 2003.
- [18] F. Göloğlu. Ternary Kloosterman sums modulo 4. *Finite Fields and their Applications*, 18(1):160–166, 2012.
- [19] J. W. P. Hirschfeld and T. Szönyi. Sets in a finite plane with few intersection numbers and a distinguished point. *Discrete Mathematics*, 97(1–3):229–242, Dec. 1991.
- [20] A. M. W. Hui, H. F. Law, Y. K. Tai, and P. P. W. Wong. Non-classical polar unitals in finite dickson semifield planes. *Journal of Geometry*, 104(3):469–493, Dec. 2013.
- [21] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*. Springer New York, New York, NY, 1990.
- [22] N. Knarr and M. Stroppel. Polarities and unitals in the Coulter-Matthews planes. *Des. Codes Cryptography*, 55(1):9–18, Apr. 2010.
- [23] G. M. Kyureghyan and A. Pott. Some theorems on planar mappings. In *Arithmetic of finite fields*, volume 5130 of *Lecture Notes in Comput. Sci.*, page 117–122. Springer, Berlin, 2008.
- [24] E. S. Lander. *Symmetric Designs: An Algebraic Approach*. Cambridge University Press, Jan. 1983.
- [25] M. Lavrauw and O. Polverino. Finite semifields. In L. Storme and J. De Beule, editors, *Current research topics in Galois Geometry*, chapter 6, pages 131–160. NOVA Academic Publishers, 2011.
- [26] K. H. Leung and Q. Xiang. On the dimensions of the binary codes of a class of unitals. *Discrete Mathematics*, 309(3):570–575, Feb. 2009.
- [27] K. H. Leung and Q. Xiang. Erratum to “On the dimensions of the binary codes of a class of unitals” [Discrete Math. 309 (2009) 570–575]. *Discrete Mathematics*, 311(18–19):2102–2103, Oct. 2011.
- [28] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.
- [29] H. Lüneburg. Some remarks concerning the Ree groups of type G_2 . *Journal of Algebra*, 3(2):256–259, Mar. 1966.
- [30] A. Pott, K.-U. Schmidt, and Y. Zhou. Semifields, relative difference sets, and bent functions. In H. Niederreiter, A. Ostafe, D. Panario, and A. Winterhof, editors, *Algebraic Curves and Finite Fields, Cryptography and Other Applications*. De Gruyter, 2014.
- [31] K.-U. Schmidt and Y. Zhou. Planar functions over fields of characteristic two. *Journal of Algebraic Combinatorics*, 40(2):503–526, Sept. 2014.
- [32] B. Segre. Ovals in a finite projective plane. *Canadian Journal of Mathematics*, 7:414–416, Jan. 1955.
- [33] R. Trombetti and Y. Zhou. Unitals in shift planes of odd order. *arXiv:1508.07279 [math]*, 2015. Submitted.
- [34] G. Weng and X. Zeng. Further results on planar DO functions and commutative semifields. *Designs, Codes and Cryptography*, 63(3):413–423, 2012.
- [35] J. Wu. Binary codes from substructures in finite projective planes. Talk given in “Wilson Fest”, a conference in honor of Rick Wilson, March 2012.
- [36] Q. Xiang. Recent results on p -ranks and Smith normal forms of some $2 - (v, k, \lambda)$ designs. In *Coding theory and quantum computing*, volume 381 of *Contemp. Math.*, pages 53–67. Amer. Math. Soc., Providence, RI, 2005.
- [37] Y. Zhou. $(2^n, 2^n, 2^n, 1)$ -relative difference sets and their representations. *Journal of Combinatorial Designs*, 21(12):563–584, 2013.
- [38] Y. Zhou. Parabolic unitals in a family of commutative semifield planes. *Discrete Mathematics*, 338(8):1300–1306, Aug. 2015.
- [39] Y. Zhou and A. Pott. A new family of semifields with 2 parameters. *Advances in Mathematics*, 234:43–60, Feb. 2013.

DIPARTIMENTO DI MATEMATICA E APPLICAZIONI “R. CACCIOPOLI”, UNIVERSITÀ DEGLI STUDI
DI NAPOLI “FEDERICO II”, I-80126 NAPOLI, ITALY
E-mail address: `rtrombet@unina.it`

DIPARTIMENTO DI MATEMATICA E APPLICAZIONI “R. CACCIOPOLI”, UNIVERSITÀ DEGLI STUDI
DI NAPOLI “FEDERICO II”, I-80126 NAPOLI, ITALY
E-mail address: `yue.zhou.ovgu@gmail.com`